



電子計算機中心
National Chung Cheng University
Computer Center

資安事件宣導

弱點掃描 網站篇

- 1 弱點掃描簡介
- 2 OWASP 簡介
- 3 2017 OWASP 網站弱點Top10



OWASP
Open Web Application
Security Project

詳見檔案內文

中華民國107年3月

一. 何謂「弱點掃描」？

何謂「弱點掃描」？

- ◆ 網路帶來便利的同時也充斥著許多的風險，有心人士散布的病毒、惡意程式等危害嚴重影響網路的安全。
- ◆ 「弱點」指的是系統因為設計不良而產生的、容易遭到入侵的缺陷或是漏洞。
- ◆ 「弱點掃描」則是指使用自動化工具對系統進行檢測，找出潛藏的系統漏洞。

二. OWASP簡介

OWASP簡介

- ◆ 全名為Open Web Application Security Project，開放網站應用程式安全計畫。
- ◆ 是一個開放社群的非營利組織，致力於改善網站應用程式的安全性。



三. OWASP 網站安全風險Top10簡介

什麼是OWASP 網站弱點Top 10？

- ◆ OWASP的知名計畫之一，調查各式各樣的網站漏洞與風險，經過整理歸納之後，所公布出**最常見的10項網站弱點**。
- ◆ 以下將介紹**前3名**(Top 1 ~ Top 3)的網站弱點。

OWASP也提供網頁弱點掃描工具

ZAP 下載網頁：

https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project#tab=Main



OWASP Top 10 Overview

2017 OWASP 網站弱點 Top 10	
Top 1	注入攻擊 (Injection)
Top 2	無效身份認證 (Broken Authentication)
Top 3	敏感資料外洩 (Sensitive Data Exposure)
Top 4	XML外部處理器漏洞 (XML External Entity, XXE)
Top 5	無效的存取控管 (Broken Access Control)
Top 6	不安全的組態設定 (Security Misconfiguration)
Top 7	跨站腳本攻擊 (Cross-Site Scripting, XSS)
Top 8	不安全的反序列化漏洞 (Insecure Deserialization)
Top 9	使用具有漏洞的元件 (Using Components with Known Vulnerabilities)
Top 10	記錄與監控不足 (Insufficient Logging & Monitoring)



網站弱點 Top 1-Injection (1/3)

1. 注入式攻擊(Injection)

- 通常發生在網頁中需要資料輸入的欄位，例如帳號、密碼的輸入欄位。
- 在輸入的字串後方夾帶資料庫的指令，由於程式設計時疏忽檢查，導致資料庫誤認為這是正常的指令而執行。
- 駭客因而達成入侵資料庫取得資料或是破壞資料庫的目的。

網站弱點Top 1-Injection (2/3)

CCU ONE
校園系統單一入口

登入 Login

帳號: 請輸入帳號

密碼: 忘記密碼

登入系統

駭客輸入有特殊字元的帳號
Ex. 「 ' or 1=1 /* 」，密碼：「任意值」

1

輸入帳號、密碼
等資料的欄位

錯誤的密碼

夾帶資料庫指令

2

123456	OR true
123456	OR '1'="1"

3

由於設計不良、系統疏忽檢查，導致即使密碼錯誤卻還是能登入帳號

網站弱點Top 1-Injection (3/3)

防護措施

- 嚴格檢查所有輸入值。
- 使用參數化查詢的方式來設計程式。
- 對輸入的字串進行過濾，清除非正當的指令或內容。
- 確實控管使用者帳號對資料庫的存取權限。

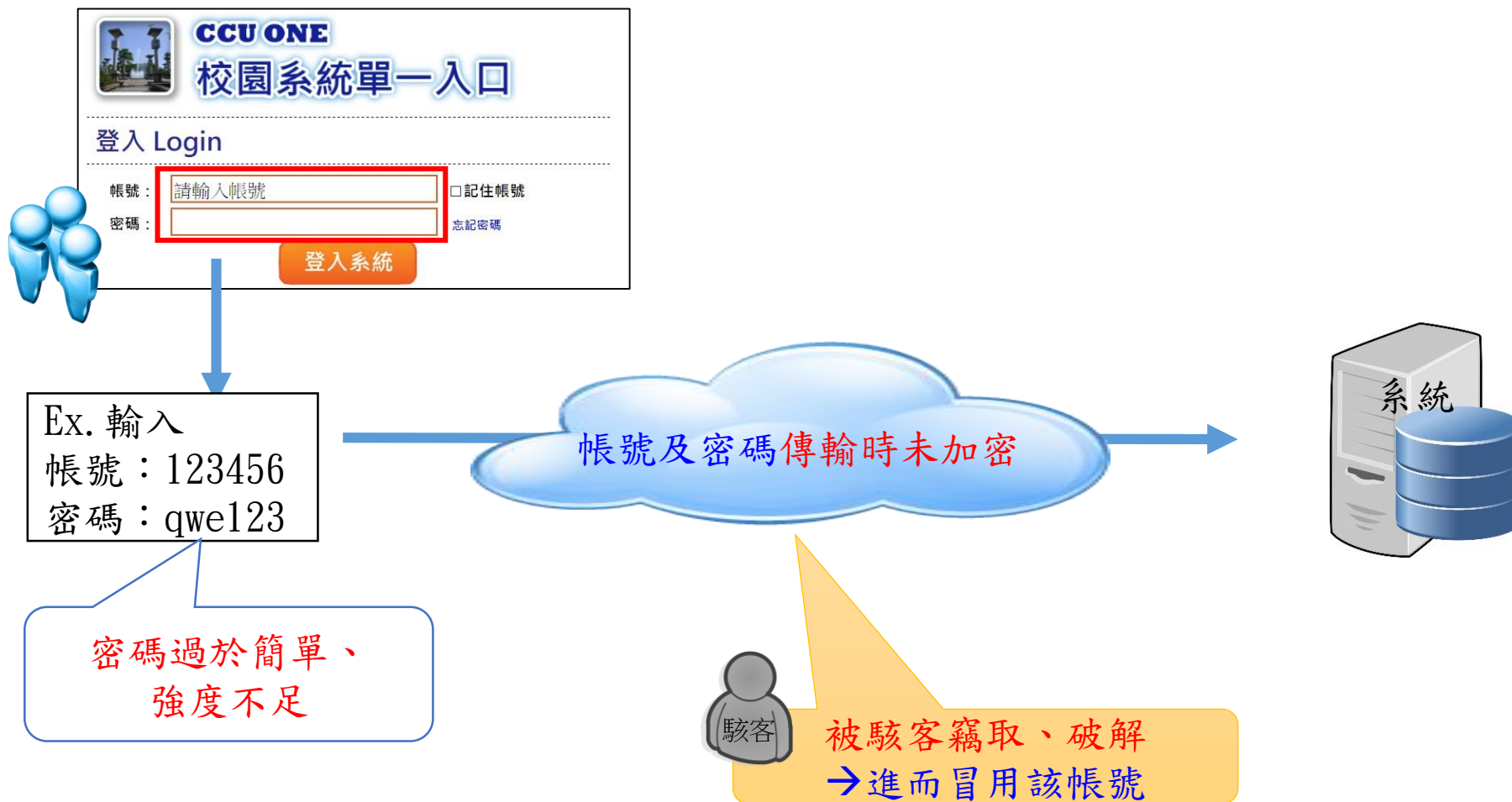
網站弱點Top 2-Broken Authentication (1/3)

2. 無效身分認證(Broken Authentication)

- 網站登入時的**身分驗證功能有缺陷**，導致駭客能夠輕易竊取相關帳密資料，進而登入並冒用該帳號。
- 網站登入時**沒有進行加密保護、密碼強度不足**等等。
- 使用者於公共電腦**沒有手動登出**系統，而是直接關閉視窗，駭客經過**一段時間**後使用同一台電腦重新開啟，卻**仍然能夠直接登入**該系統。

網站弱點Top 2-Broken Authentication (2/3)

※以下採本校網站畫面進行說明



網站弱點Top 2-Broken Authentication(3/3)

防護措施

- 確保密碼以及其他資訊透過**加密**的方式傳輸到網站資料庫。
- 確保身份憑證有透過**加密**、**雜湊(hash)**等方式進行保護。
- 設定完善的**自動登出(Time out)**機制。
- 添加**密碼強度驗證**功能、**密碼定期更換**機制。

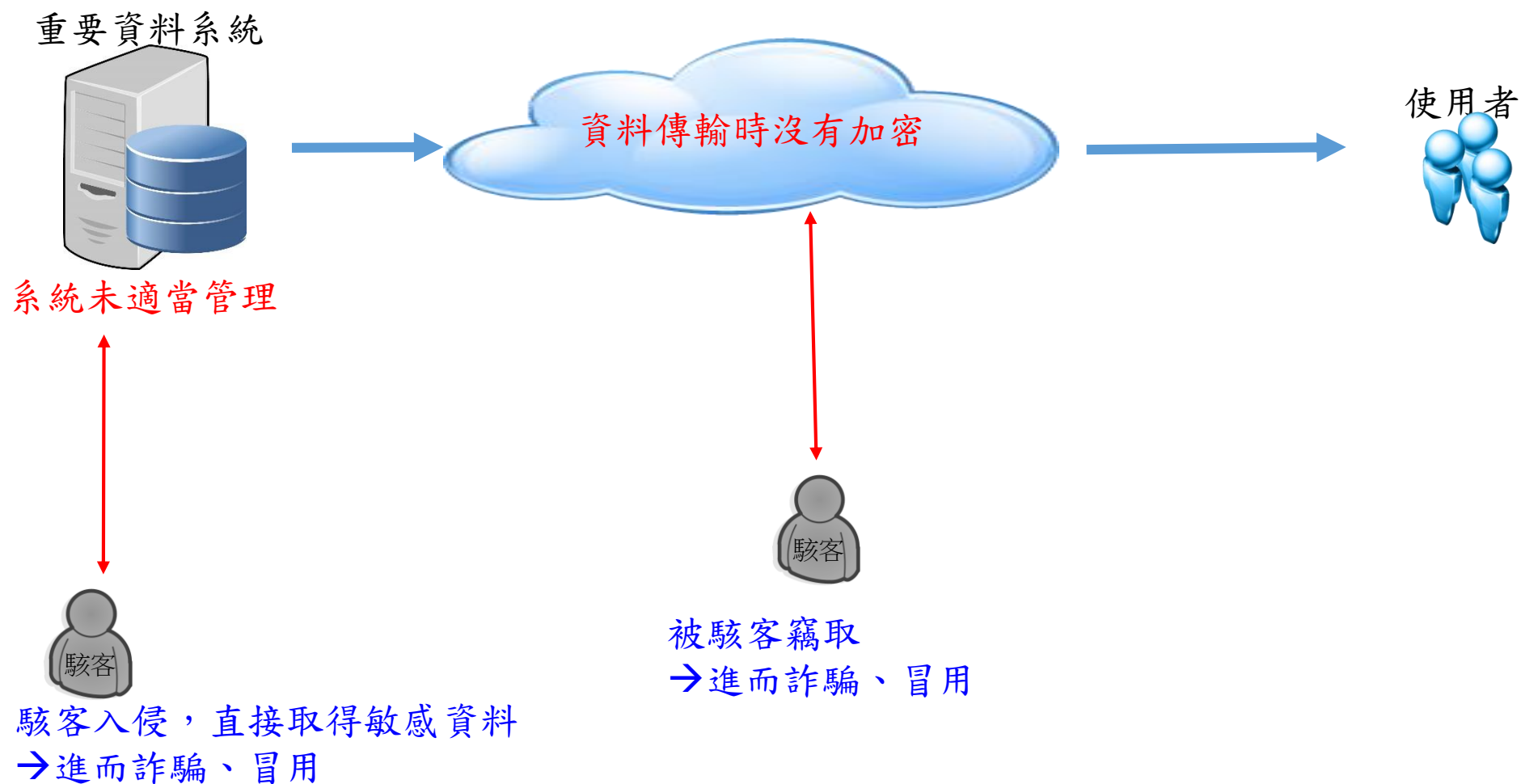


網站弱點Top 3- Sensitive Data Exposure(1/3)

3. 敏感資料外洩(Sensitive Data Exposure)

- 敏感資料意指容易遭到有心人士利用的個人資料，例如金融資訊、醫療保健數據等等。
- 網站對於這些敏感資料的保護度不足，使得駭客入侵系統後，能夠輕易地竊取資料。
- 駭客進而達成詐欺、冒用身分等犯罪行為。

網站弱點Top 3- Sensitive Data Exposure(2/3)



網站弱點Top 3- Sensitive Data Exposure(3/3)

防護措施

- 使用SSL加密連線進行資料傳輸。
- 以加密、雜湊(hash)等方式保存敏感資料，例如帳號密碼。
- 檢查系統防火牆規則設定，限制所需的連接埠，並定期查看內部是否有對外大量不同目的 IP 之異常連線，與帳號活動。



電子計算機中心
National Chung Cheng University
Computer Center

感謝閱讀

資訊安全宣導

資料參考來源

- OWASP https://www.owasp.org/index.php/Main_Page
- OWASP ZAP弱點掃描工具下載頁面：
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project#tab=Main
- 資安人
https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=7290
https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=7754
- OpenFoundry電子報
<https://www.openfoundry.org/tech-column/2354>
- MMDays 資訊安全雜談
http://mmdays.com/2013/12/11/owasp_top_10/
- iThome 資安新聞
<https://www.ithome.com.tw/news/118411>